DEPARTMENT OF THE NAVY
NAVAL HOSPITAL
BOX 788250
MARINE CORPS AIR GROUND COMBAT CENTER
TWENTYNINE PALMS, CALIFORNIA 92278-8250

IN REPLY REFER TO:
NAVHOSP29PALMSINST 5540.2A
Code 0106
3 April 1998

NAVAL HOSPITAL TWENTYNINE PALMS INSTRUCTION 5540.2A

From: Commanding Officer

Subj: COMMAND SECURITY PROGRAM

Ref: (a) OPNAVINST 5530.14B
(b) NAVHOSP29PALMSINST 6700.10C
(c) SECNAVINST 5500.4G
(d) CCO P1630.7C
(e) SECNAVINST 1740.2D
(f) SECNAVINST 5370.2J
(g) MILPERSMAN Article 1850140
(h) OPNAVINST 5510.1H
(i) OPNAVINST 5239.1A
(j) SECNAVINST 5239.3
(k) NAVHOSP29PALMSINST 6010.9C
(l) NAVHOSP29PALMSINST 5530.3A
(m) OPNAVINST 11320.23E
(n) NAVHOSP29PALMSINST 6010.8B
(o) Joint Commission, Comprehensive Accreditation Manual for Hospitals: The Official Handbook, Current Edition

1. Purpose. To publish policy and set forth standards for security measures to safeguard patients, staff, visitors, property and sensitive information at Naval Hospital, Twentynine Palms and its clinics as per references (a) through (o).

2. Cancellation. NAVHOSP29PALMSINST 5540.2.

3. Background. Naval Hospital, Twentynine Palms is a resident command located on the Marine Corps Air Ground Combat Center (MCAGCC). To provide the security force required in reference (a), this command relies on the Provost Marshall's Office (PMO) as addressed in reference (d).

4. Action

a. The Commanding Officer shall appoint the Security Officer, Security Manager, Personnel Security Officer, Top Secret Control Officer and the Classified Material Control Officer in writing.

b. The Security Officer shall be responsible for all physical security and loss prevention programs.

c. The Security Manager shall be the principal advisor on information and personnel security in the command.

d. The Personnel Security Officer shall ensure that all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and briefed.

e. The Top Secret Control Officer shall:

(l) Ensure all Top Secret information is controlled by direct personal contact.

(2) Ensure no Top Secret material is stored at this command.

f. The Classified Material Control Officer shall:

(1) Ensure compliance with accounting and control requirements for classified material.

(2) Ensure emergency removal for classified material.

g. Head, Management Information Department (MID) shall:

(l) Be assigned as the Information Systems Security Officer.

(2) Be responsible for developing and implementing Information Systems (IS) security.

h. Directors and Department Heads shall:

(1) Familiarize themselves with the contents and requirements of enclosures (l) through (3).

(2) Make their personnel available for training as scheduled.

5. Applicability. This instruction is applicable for all personnel aboard this command and its clinics.

6. New or Revised Forms. Command Authorization for Search and Seizure, OPNAV 5527/9; Affidavit for Search Authorization, OPNAV 5527/10; Department of Navy Evidence Tag, OPNAV 5527/A and B; Evidence/Property Custody Document, NAVHOSP29PALMS Form 3440/03 (Rev. 2/94) and Security Container Information Card, SF-700 may be obtained from Central Files Department.

R. S. KAYLER

Distribution:
List A

TABLE OF CONTENTS

CONTENTS PAGES

CONTENTS PAGES

Chapter 11 - Bomb Threat Procedures

Figure

Chapter 12 - Terrorist Threat Procedures

Chapter 13 - Infant and Pediatric Security

Figure

Chapter 14 - Classified Information and Personnel Security System

Chapter 1

INTRODUCTION

1001. Purpose. To establish policy, procedures and requirements for the Physical Security and Loss Prevention Program at Naval Hospital Twentynine Palms. Specifically, this chapter covers:

a. Responsibilities for physical security and loss prevention.

b. Measures to assist in identifying, analyzing, reducing and eliminating losses of government property and to improve physical security.

c. The physical security of resources and assets and is intended to provide a comprehensive physical security program as required by reference (a).

1002. Action

a. The Commanding Officer shall:

(l) Be responsible for physical security.

(2) Appoint a Security Officer.

(a) Appointment must be writing.

(b) Be qualified as per reference (a).

(3) Designate restricted areas as required by reference (a).

(4) Provide sufficient resources, training, staff assistance and authority to the Security Officer to allow for the implementation, management and execution of an effective physical security and loss prevention program.

b. Physical Security Review Committee (PSRC) shall:

(l) Be convened under the cognizance of the Board of Directors, pursuant to reference (k).

(2) Meet quarterly and perform the duties as described in reference (a).

(3) Be chaired by the Security Officer.

c. The Security Officer shall:

(l) Report to the Commanding Officer on all security matters.

(2) Assist the Commanding Officer in the determination of the adequacy of the Command Physical Security and Loss Prevention Program by identifying those areas in which improved security measures are required.

(3) Be responsible for the command's physical security, anti-terrorism, and loss prevention programs by:

(a) Identifying the asset requiring protection, assessing the threat, committing resources and determining jurisdiction and boundaries.

(b) Detecting efforts to wrongfully remove, damage or destroy property by employing a security force sufficient to protect, react to and confront situations and circumstances which threaten personnel and property.

(4) Ensure all loss reporting, trend analysis and investigative requests are completed.

(5) Ensure that all losses and gains, inventory adjustments, and surveys of property are reported, pursuant to references (b) and (c).

(6) Forward all investigations requiring PMO, Naval Criminal Investigative Services (NCIS) and/or Criminal Investigative Department (CID) attention to the appropriate agency.

(7) Monitor disciplinary, administrative, and corrective procedures applicable to members found responsible for losses.

(8) Conduct an annual physical security survey.

(9) Request external in-depth studies or physical security inspections.

(10) Provide a basis for the orderly improvement of this command's Physical Security and Loss Prevention Program.

(11) Conduct the initial investigation of motor vehicle accidents occurring within the jurisdictional boundaries of the command that involve vehicles assigned to the command. The Accident Investigations Branch, PMO, MCAGCC will be notified of all such accidents.

(12) Be liaison to the MCAGCC Physical Security Officer regarding matters of physical security.

(13) Ensure training on physical security and loss prevention is provided during Command Indoctrination and Annual Training.

d. The Chief Master at Arms (CMAA) shall:

(l) Immediately investigate incidents involving criminal or disciplinary matters.

(2) Notify the Security Officer as to the status and findings of investigations.

(3) Serve as a liaison between the command and other law enforcement agencies.

(4) Assume the duties of the Command Security Officer in his absence.

(5) Maintain records and files of:

(a) Evidence taken into custody

(b) Investigative files

(c) Disciplinary records

(6) Serve as the Command Evidence Custodian.

(7) Be responsible for the preparation of personnel packages for use in Courts-Martial and Article 15, Uniform Code of Military Justice (UCMJ) cases.

(a) Ensure personnel are rendered their rights provided by Article 31 of the UCMJ.

(b) Ensure packages are reviewed by the Security Officer and Director for Administration before being forwarded for action.

(8) Conduct at least one external security inspection of the command on normal work days.

e. Head, Education and Training shall:

(l) Provide adequate time at Command Indoctrination and Annual Training for security briefings.

(2) Security Briefings will address:

(a) Processes for minimizing security risks for personnel in security sensitive areas;

(b) Emergency procedures followed during security incidents; and

(c) Processes for reporting security incidents involving patients, visitors, personnel, and property.

(3) Maintain training records of personnel attending security training.

1003. Security Team. This command's Security Team consists of a Security Officer and a collateral duty CMAA. The Officer of the Day (OOD), Mate of the Day (MOD) and other watchstanders may be used to augment the security team as the situation dictates. MCAGCC PMO shall provide a security force when requested.

1004. Internal Security

a. All security violations and discrepancies will be reported in the Command Journal.

b. Office spaces will be secured at the close of normal working hours, weekends and holidays except when personnel need to perform their duties.

c. Internal doors to offices containing sensitive or classified material will only be secured after material has been

properly secured. Security checks will be made by the OOD/MOD twice during each 24 hour shift and the results recorded in the Command Journal.

d. When not in use, all vaults and safes will be closed and locked.

e. Departments that handle service or health records will ensure that records are placed in adequate locked storage cabinets and all doors to the record storage areas are secured prior to leaving their work center.

f. When a space is assigned a dual occupancy by two or more departments, the senior Department Head will assume responsibility for the security of that space.

g. If forced entry of a space is suspected, the Security Officer or Officer of the Day will be notified immediately.

(a) The immediate area will be isolated and not disturbed until relieved by the Security Officer or the Officer of the Day.

(b) No further entry into the space is authorized.

(c) Nothing is to be removed from or placed inside the space.

1005. External Security

a. The PMO is responsible for patrolling all common areas (streets, roads, parking areas, etc.) surrounding the Naval Hospital.

b. After normal working hours, weekends and holidays, the OOD and MOD are responsible for security rounds of all buildings under the cognizance of this command.

(l) Conditions of all exterior lighting, doors, and windows will be noted, with discrepancies reported to the Security Officer the following work day. The OOD will indicate discrepancies on the OOD Checklist and report those discrepancies the next day to the Director for Administration and the Executive Officer.

(2) When required, work requests shall be completed by the Security Officer and forwarded to facilities Management Department for action.

c. Doors shall not be propped open and left unattended.

d. All exterior doors except the main entrance and emergency room will be secured at 1800 on work days and will be opened at 0530. Doors will remain secured on weekends and holidays.

Chapter 2

KEY AND LOCK CONTROL PROGRAM

2001. Purpose. To prescribe policies and procedures for the Command Key and Lock Control Program.

2002. Background. The Naval Hospital and Military Sick Call keying system is a master-keyed system designed for door keys to allow access to specific spaces. Locking devices for personal use, desks, lockers and file cabinets are not covered by this program.

2003. Action

a. The Security Officer shall be responsible for the Command Key and Lock Control Program.

b. The Command Key Control Officer shall:

(l) Be appointed in writing by the Commanding Officer.

(2) Maintain a master inventory of keys assigned to hospital staff and contractors.

(3) Conduct semi-annual key inventories and maintain inventory files.

(4) Coordinate lock maintenance and rotation.

(5) Approve/Disapprove all requests for key or lock changes and forward the requests to the Safety Manager for review.

(6) Investigate reports of lost or recovered keys. PMO or NCIS will be notified of the loss of any master, sub-master, pharmacy, material management, mail room, or collection agent room key.

(7) Budget for all aspects of the Key Control Program.

(8) Conduct an annual review of the Key Control Program.

c. Department Heads shall ensure all department duty keys are controlled and losses reported to the Security Officer immediately.

d. All personnel shall:

(l) Report lost, damaged, or stolen keys to their Department Head.

(2) Submit key and lock requests to the Security Officer via their Department Head.

(3) Not duplicate any government key by any means other than through the Department Key Custodian.

(4) Surrender any keys found to the Security Officer.

(5) Surrender all keys to the Security Officer prior to transfer from the department. *KEYS SHALL NOT BE TURNED OVER TO OTHER STAFF MEMBERS.*

(6) Responsible for preventing the unauthorized use of command keys.

2004. Key Control

a. Duplicate Key Control. Duplicate keys will be secured in the Operating Management Department as required by reference (a).

b. Duplication of Keys. MCAGCC's locksmith is the only person authorized to make and duplicate keys. Keys will not be duplicated by a commercial vender. All requests for key duplication must be processed through the Security Officer.

c. Key Accountability. Continuous accountability of keys is required. The Security Officer shall maintain a system showing keys on hand, keys issued, to whom, date and time the keys were issued and returned, and the signatures of persons issued or returning the keys.

d. Key Issuance. Keys will only be issued to persons needing access to locked areas to conduct official duties. The issuance of keys will be limited to a minimum number required to perform efficient routine operations. Keys will not be issued merely for convenience.

2005. Lock Control

a. Maintenance. MCAGCC's locksmiths are the only personnel authorized to perform maintenance on locks.

b. Procurement of Locks. All locking devices must be approved by the Security Officer and Safety Manager prior to procurement.

c. Cipher and Safe Locks. Will be changed at least annually, upon change of custodian(s), compromise or suspect of compromise.

d. Electronic Card Access Locks. Sensitive areas throughout the command will be equipped with electronic locks. Cards will be issued individually to staff members. Electronic locks will have tracking capability to determine who entered, date and time. Access cards will be turned over to the Security Officer on transfer or departmental change.

Chapter 3

PERSONNEL ACCESS, IDENTIFICATION AND MOVEMENT

3001. Purpose. To describe policies and procedures for the access, movement, and identification of personnel working or visiting the command.

3002. Policy

a. Access to the hospital will be granted to those persons who:

(l) Have been officially recognized to conduct business within the command, displaying the Command Photo Identification Badge.

(2) Are hospital or patients' visitors.

(3) Are Emergency Response Personnel in the performance of their duties.

b. Loitering will not be permitted.

c. Casual visiting of employees by non-employees at work will not normally be permitted except by specific permission of the employee's immediate supervisor.

d. Entry during normal working hours is not restricted.

(l) After normal working hours, entry will be restricted to the hospital only through the Information Desk Lobby and Emergency Medicine Department.

(2) All other entrances will normally be secured and alarmed by 1800 and remain secured until 0600 the next morning.

e. All members of the hospital are issued a Photo Identification Badge upon reporting. The Badge must be displayed at all times while inside the hospital or Military Sick call.

3003. Security Areas. Only the Commanding Officer may designate "restricted" areas.

a. Level Two Access Areas

(l) Material Management Storeroom

(2) Management Information Department

(3) All Electrical, Mechanical and Communications Rooms

(4) OOD/Information Desk

(a) Access to these areas will be controlled by departmental personnel and the OOD.

(b) After hours, all persons entering and leaving these spaces must be logged in the Ingress/Egress logs by the OOD.

(c) Visitors shall not be left unescorted.

(d) Security rounds will be conducted once every eight hours.

b. Level One Access Areas

(l) Pharmacy Department

(2) Mail Room

(3) Collection Agent's Office.

(4) Pharmacy vault located in Materials Management.

(a) Access to these areas will be controlled by departmental employees and the OOD.

(b) After hours, all persons entering and exiting these spaces will be logged in the Ingress/Egress logs by the OOD.

(c) Visitors shall not be left unescorted.

(d) After hours, security rounds will be conducted once every eight hours.

c. Naval Hospital and Outlying Buildings, except as noted in this instruction, are non-restricted areas.

3004. Access Criteria

a. Assigned Personnel. All personnel assigned to the Naval Hospital shall meet MCAGCC requirements for access and must present their Department of Defense identification card, upon request by the Security Officer, CMAA or watchstanders.

b. Military Staff Personnel. Military hospital staff may enter the facility at any time in the performance of their duties, however, the hospital Photo Identification Badge must be displayed.

c. Dependent and Retired Personnel. Dependents with a valid Uniformed Services Identification and Privilege Card (USIPC - DD Form 1173) and retired military personnel with a valid Armed Forces Identification Card (DD Form 2 Retired) may enter the hospital after normal working hours to use the Emergency Medicine and Pharmacy Departments, or to visit patients.

d. Children of military personnel (active, reserve and retired) under the age of ten years or without a USIPC Card must be accompanied by an adult.

e. Civilian Employees. Civilian employees will not be permitted entry into the hospital between 2000 and 0600, except in the performance of their duties, to use the Emergency Medicine Department or to visit patients.

3005. Naval Hospital Visitors

a. Law Enforcement and Investigative Agents

(l) Agents or representatives of Emergency Services, military law enforcement or investigative agencies will be admitted upon presentation of satisfactory identification when performing official duties.

(a) The agent or representative will be directed to the Security Officer during normal working hours or to the OOD after normal working hours, and on weekends and holidays.

(b) Military law enforcement agents conducting business in the Emergency Medicine Department need not report to the OOD prior to conducting their duties.

(2) Emergency Medicine Department personnel shall ensure that the OOD has been notified when any law enforcement personnel are on board, and the nature of their visit.

b. Business Visitors

(1) Since all individuals of the hospital generally have sufficient opportunity to conduct private business during off-duty hours, it is this command's policy that solicitors and agents of commercial concerns are not permitted to enter the hospital to conduct private business with employees individually as per reference (e).

(2) The Commanding Officer may authorize visits for the purpose of soliciting insurance, or for the selling of mutual funds or securities. However, information must be provided to employees in group form. At no time will solicitors be authorized one-on-one contact with employees. If employees are interested in products solicited, they may arrange a meeting after duty hours.

(3) Information Desk personnel and watchstanders will take the following action when a commercial agent or solicitor desires entrance.

(a) Obtain the name of the agent/solicitor and firm represented.

(b) Confirm by telephone that the visit has been scheduled and authorized by the Command Suite. A representative of the Commanding Officer will escort the individual(s) to the scheduled meeting area.

(c) Issue official visitor badges and make appropriate journal entries.

(4) All authorized agents must have been cleared through the MCAGCC Staff Judge Advocate's (SJA) Office. They must present credentials from SJA upon request.

(5) Representatives of the news media may be allowed access only after clearance by the MCAGCC Public Affairs Officer, the Commanding General, and the Naval Hospital Public Affairs Officer.

c. Social Visitors

(l) Groups and organizations desiring to visit for educational or informational purposes will be permitted entry upon approval of the Commanding Officer or Executive Officer. Prior arrangements for the visit must be made with the Public Affairs Officer and the Security Officer. In the case of visits to specific departments, a representative from the specific department will be designated by the Department Head to escort the visitor.

(2) Distinguished persons (governors, flag officers, senators, congressmen, senior government representatives, etc.,) will be admitted without delay and will be escorted by a command representative. The Information Desk personnel or the OOD shall immediately notify the Commanding Officer of the arrival of distinguished persons.

3006. Identification and Control

a. Military personnel shall carry the Department of Defense (DoD), Armed Forces of the United States Identification Card, DD Form 2N, on their person at all times and present it upon request by authorized personnel. Photo Identification Badge shall also be displayed.

b. Civilian personnel assigned to the hospital are issued U. S. Government Identification Cards (OF-55) by the Human Resources Officer (HRO). This card must be in their possession at all times and must be presented upon request by authorized personnel. This identification card is the property of the U. S. Government and must be surrendered upon termination of employment. Photo Identification Badges shall be displayed at all times.

3007. Debarment

a. Individuals who are barred from the hospital by the Commanding General, MCAGCC will not be permitted to enter the hospital except in the case of a bonafide emergency.

b. Persons showing evidence of being under the influence of alcohol or drugs will not be allowed access to the hospital except in cases that require medical attention.

c. Individuals participating in picketing, demonstrations, sit-ins, protest marches and political speeches may be removed and barred from the hospital. Guidance should first be sought from the SJA's office.

(l) Distribution at the hospital of materials such as pamphlets, handbills, fliers, newspapers, magazines, leaflets, petitions, etc., is prohibited except through the regularly established and approved distribution outlets or unless prior approval is obtained from the Commanding Officer.

(2) Offensive or degrading signs, placards or stickers, whether handcarried, affixed to or painted upon buildings, conveyances, or other objects, will be prohibited only after consultation with SJA.

d. No one shall enter Naval Hospital to conduct activities which are prohibited by this Manual. Such entry will constitute a violation of Title 18, United States Code, Section 1382, which provides in part that, "Whoever, within the jurisdiction of the United States, goes upon any military... reservation,...station or installation, for any purpose prohibited by law and lawful regulation...shall be fined not more than five hundred dollars ($500.00) or imprisoned not more than six months, or both."

e. The following are procedures for barring person(s) from the hospital:

(l) Debarment letters will only be issued by the Commanding General, following consultation with the SJA.

(2) Debarment letters will specify the reason for the action, the specific areas of prohibited access and the period of time the debarment action is effective. Any complaints, subpoenas or temporary restraining orders or other actions concerning debarment letters shall be referred to the SJA.

3008. Prohibitions. The following activities are prohibited aboard this command:

a. Agents, salesmen or peddlers are strictly prohibited from entering any storeroom unescorted.

b. Agents are not permitted to address meetings, classes, mass formations or any other assembly unless authorized by the Commanding Officer.

c. No command personnel, either for themselves or for an agent will:

(l) Engage in trade or introduce any article.

(2) Bring into the command any salesman, distributor or vendor, except when authorized by the Commanding General. The Commanding Officer must authorize such activities at the hospital.

3009. Reporting. Any person who discovers a peddler, agent, vendor or salesman, either military or civilian, transacting business at the hospital without proper authority, will report the circumstances to the Security Officer or the OOD immediately.

3010. Commercial Solicitation

a. Reference (f) sets forth the policies pertaining to standards of ethical conduct governing all personnel of the Department of the Navy.

b. Agents must have in their possession a valid business pass issued by PMO.

c. All agents, salesmen, or peddlers shall be escorted to:

(l) Material Management Department

(2) Head, Pharmacy Department for pharmaceutical displays or product introduction.

(3) The Department Head that has the scheduled appointment for visits of noncontractual nature.

d. Head, Material Management Department will be responsible for identifying vendors that provide products or services on a regular scheduled basis to the command, in

writing, to PMO to request issuance or cancellation of regular vendor decals.

3011. Fund Raising by Private Organizations. Private organizations of a civic, social or fraternal nature, which serve to enrich military life, will normally be approved to conduct fund raising at the hospital. Approval to conduct such activities will be subject to reference (f) and the following:

a. Activities that conflict or compete with authorized functions of nonappropriated funds instrumentalities, i. e., Marine Corps Exchange, Special Services, and the Club System, will not be approved. Determination of conflicts or competition rests with the Executive Officer.

b. Each proposed fund-raising activity will be approved by the Commanding Officer via the Executive Officer and Director for Administration.

Chapter 4

SEIZURE AND HOLDING OF CONTRABAND PROPERTY OR EVIDENCE

4001. Purpose

a. To declare and define property considered contraband and prohibited to possess aboard the hospital.

b. Establish policies in collecting, storing and disposing of property.

4002. Definitions

a. Contraband is property which is defined by federal and state statutes as illegal to possess and subject to forfeiture upon seizure. For specific descriptions of contraband, refer to reference (a).

b. Prohibited is property, other than contraband, which is prohibited by order of the Commanding Officer or higher directives.

4003. Searches

a. Authority to search

(l) The Commanding Officer may order searches of:

(a) All military personnel under the authority of the Commanding Officer.

(b) All personal property of persons on or entering the hospital, on a random basis.

(c) All properties under the authority of the Commanding Officer.

(d) Civilian employees and their property.

(2) If the Commanding Officer is absent from the command, the Acting Commanding Officer may authorize searches.

(3) The Command Duty Officer (CDO) possesses no inherent power to authorize a search.

(a) The CDO may exercise general command authority if the Commanding Officer and the Acting Commanding Officer are absent or unavailable.

(b) If the CDO makes the decision to authorize a search, the circumstances will be documented in full detail, including the reason the Commanding Officer could not act upon the decision.

b. Command Authorized Search

(l) Prior to ordering a command authorized search of persons or property, the officer ordering the search must be assured that probable cause exists. Probable cause is when a reasonable person would believe that a offense has been committed and that a particular person(s) committed that offense.

(2) Sources of information must be reliable and correct. The information may consist of:

(a) The repetition of facts or statements by someone who does not have first-hand knowledge, but by virtue of his reputation, has proven to be honest and trustworthy.

(b) Someone telling what they saw or found.

(3) The reliability of the absent informer must be determined if statements or observations of persons not physically present are to be relied upon.

c. Consent to Search. During an investigation, the suspect may be asked permission to conduct a search of self and property. This consent must be documented on a Permissive Authorization for Search and Seizure (OPNAV 5527/16), and witnessed.

d. Plain View Search. Evidence which is found in plain sight.

4004. Seizures

a. Consult with MCAGCC SJA prior to initiating any search, if possible, to ensure all legal requirements are met.

b. Contact PMO and request a representative be present prior to conducting any search.

c. Personnel conducting a lawful search are to seize all items found which fall within the following categories:

(l) Evidence of an offense in violation of the UCMJ.

(2) Instrumentalities to commit an offense or to effect the escape of the offender.

(3) Evidence suggesting the identity of the offender.

(4) Contraband.

d. Any contraband or prohibited property discovered will be immediately safeguarded.

e. If not already on board, PMO will be contacted for recovery.

f. Under no circumstances will suspected evidence be touched, handled or tampered with, except in extreme emergency, and then only to the minimal amount possible pending arrival of PMO.

4005. Custody of Evidence. MCAGCC PMO stores and maintains all evidence.

Chapter 5

PROTECTION OF PERSONS AGAINST ACTS OF AGGRESSION

5001. Purpose. To establish procedures for anticipating and dealing with violence.

5002. Background. This command has the responsibility of providing adequate security measures to safeguard the lives and property of the patients, staff and visitors. Standards of the Joint Commission for Accreditation of Healthcare Organizations (JCAHO) require, in part, that measures be taken to produce safe policies and practices and to eliminate or reduce possible hazards to all persons.

5003. Policy. Code “Romeo” is the announcement/code used.

a. This command will make every effort to prevent or address acts of violence presented to patients or staff of this command.

b. When addressing a violent patient, refer to reference (a).

5004. Action

a. Personnel witnessing a violent or aggressive act will:

(l) Notify the OOD Desk and have them announce “Code Romeo” over the Public Address System.

(2) Provide the location and other pertinent details necessary for assessment of the relative danger, i.e., firearms or other weapons, violent individuals(s), or group, etc.

b. Personnel at the OOD desk shall contact the Security Officer or CMAA during normal working hours and the OOD after working hours indicating Code Romeo was called and location.

c. Security Officer, CMAA, or OOD shall:

(l) Make the necessary initial assessment.

(2) Report all acts of violence or aggression to the Director for Administration, during normal working hours.

(3) Request support from PMO to subdue and restrain individual(s) if additional assistance is required.

(4) In the event of a Civil Disturbance or demonstration, the following actions will be taken:

(a) Notify the Commanding Officer, Executive Officer, Director for Administration, and MCAGCC's Command Duty Officer.

(b) Secure all entrances to the hospital and post personnel at each entrance.

(c) Notify and coordinate assistance with PMO.

(d) Isolate and secure the area of the disturbance or demonstration, if possible.

(e) Recall all off-duty personnel from the Bachelor Enlisted Quarters (BEQ).

(f) Keep the Commanding Officer apprised of the situation at all times and as it progresses.

Chapter 6

SECURITY OF PATIENTS IN A DISCIPLINARY STATUS

6001. Purpose. To establish a policy for the custody and control of patient personnel who are in a disciplinary status.

6002. Background. The Command may be tasked to provide medical care of patients who are in a disciplinary status. Personnel in a disciplinary status fall into two categories;

a. Prisoners serving in a sentence imposed by competent authority.

b. Personnel awaiting disciplinary action.

6003. Policy

a. Confinement or other controls adopted will always be consistent with, but secondary to, the examination and treatment of the patient.

b. Prisoners or personnel awaiting disciplinary action will not be admitted for elective surgery except when approved by the Clinical Department Head. If admitted, prompt action will be taken to ensure these personnel are returned to a duty status as soon as possible after completion of treatment.

6004. Action. The control of disciplinary cases will be accomplished as follows:

a. Navy Personnel. Comply with reference (g) regarding the reporting of disciplinary status of patients.

b. Marine Corps Personnel. Commanding Officers of Marine Corps personnel are responsible for notifying the Commanding Officer, in writing, if there is disciplinary action pending in a patient's case. The absence of this information usually results in no action being taken to restrict the Marine to this Command. If restraint/restriction is required, security escort personnel must be furnished by the Marine's Commanding Officer.

c. Detention Cell Confinees

(l) When detention cell confinees require hospitalization, their release will be effected by the confinee's Commanding Officer. In cases occurring after normal working hours, the confinee's CDO may authorize the release.

(2) The CMAA will contact the individual's parent organization Commander for the purpose of establishing security measures and request security guards if deemed necessary based on the individual's status and charges.

(3) Upon completion of hospitalization, the individual will be discharged to the parent command for appropriate disposition.

(4) Prisoners reporting for outpatient care will be accompanied by a chaser.

d. Inpatient Nursing Staff shall:

(l) Notify the CMAA upon admitting a patient who is a prisoner or in a restrictive status.

(2) Muster patients who are a prisoner or in a restrictive status at 0800, 1200, 1600, 2000 and 2400 daily.

(3) Report to the Security Officer, during normal working hours, and to the OOD after normal working hours, the status of prisoners or restricted patients.

e. Patients in a Restricted Status shall:

(l) Muster with Inpatient Nursing Department personnel at 0800, 1200, 1600, 2000 and 2400 daily.

(2) Be accompanied by hospital staff personnel when leaving the nursing unit.

(3) Not be allowed at any recreational activity.

(4) Be authorized chapel visits when accompanied by authorized personnel.

Chapter 7

Dangerous Weapons

7001. Purpose. To promulgate policy concerning dangerous weapons aboard this activity.

7002. Policy on Carrying Firearms Inside Naval Hospital

a. Law enforcement officials, including military policemen and security escorts, *in the performance of their duties*, may retain their weapons and ammunition.

b. Patients must surrender their weapons upon entry to the hospital. If unit members accompany the patient, the unit will take custody of the weapons.

c. The CMAA or MOD shall take custody and retain weapons of visitors and patients, if unit members are not present, upon entering the hospital. PMO will be immediately notified to take custody of the weapons.

7003. Definitions

a. Firearms. Pistols or rifles that fire projectiles by gas or compressed air.

b. Weapons firing dangerous missiles. Weapons capable of launching dangerous missiles including bows, crossbows, and sling shots. The type of missiles considered dangerous are arrows, bolts, darts, pellets, and missiles capable of inflicting serious injury.

c. Concealed weapons are any dangerous weapons such as firearms, blackjacks, saps, brass knuckles, knives, clubs, razors or exposed blades thereof, carried on the person for use as a weapon.

d. Spring or gravity activated knives. Knives with spring or gravity activated blades commonly known as switchblades or stilettos are specifically forbidden. Their possession is a violation regardless of length, whether concealed or not.

7004. Action

a. Head, Emergency Medicine Department shall:

(l) Ensure that all unconscious patients brought into the Emergency Medicine Department are inspected for weapons.

(2) Ensure that weapons are turned over to a representative of the patient's command or to PMO.

(3) Notify the CMAA or MOD if a representative of the patient's command or PMO is not onboard to assume custody.

b. CMAA or MOD shall:

(l) Standby and wait for PMO to assume custody of any weapon or ammunition found on a patient.

(2) Record identification information to whom the weapon is released to.

Chapter 8

LOSS PREVENTION

8001. Purpose. To provide procedures for the protection of hospital assets.

8002. Policy. It is the policy of this command that all personnel shall protect government property under their charge from theft, misuse, abuse and waste by:

a. Loss analysis to help identify trends and patterns of losses.

b. Physical security of all internal and external spaces.

c. Resource utilization controls to preclude misuse, abuse, misappropriation and excessive waste.

d. Increased awareness through education of the importance of security and loss control at all management levels.

e. Discipline, financial responsibility and accountability of personnel for equipment and supplies and the physical security of work areas under their cognizance.

8003. Action

a. Loss Prevention Subcommittee (LPS) shall:

(l) Function as a subcommittee of the Physical Security Review Committee (PSRC) and be chaired by the Security Officer.

(2) Meet at least quarterly to review and tabulate losses and monitor action taken.

(3) Submit minutes for approval to the PSRC.

b. The Security Officer shall:

(l) Ensure that Missing, Lost, Stolen or Recovered (M-L-S-R) Government Property Reports are submitted as instances warrant as required by reference (c) and this manual.

(2) Provide a consolidated report of M-L-S-R government property to the LPS. This report shall contain such information as type of property reported missing, lost, stolen, or recovered, department work center held accountable, date discovered missing, date reported to the security division as missing, value of the property, whether the property is categorized as M-L-S-R (as defined in reference (c)) and date reported to the proper investigative agency.

(3) Assist Department Heads in evaluating physical security of their respective spaces, using reference (a) as a guide, and recommend improvements.

(4) Conduct local investigations of thefts of government property in conjunction with CID or NCIS, as appropriate.

(5) Conduct a security survey of the hospital at least annually and report the findings to the Board of Directors (BOD). Retain a copy of this survey for the next Inspector General inspection cycle or a minimum of three years, whichever is greater as required by reference (a).

(6) Attend the MCAGCC Security and Loss Prevention Council Meeting each fiscal quarter as an active participating representative of the hospital.

c. Head, Material Management Department shall:

(l) Establish and monitor usage rates for consumable supplies; reporting problems to the BOD via the Security Officer.

(2) Promptly report Missing, Lost, Stolen or Recovered (M-L-S-R) government property to the Security Officer.

(3) Ensure procurement of all locking devices are approved by the Security Officer and Safety Manager and follow the guidelines of reference (a).

d. Command Equipment Manager shall:

(l) Maintain an accountability system for both minor and plant property.

(2) Ensure that all minor and plant property are electro-mechanically engraved or embossed to deter theft.

e. Department Heads shall:

(1) Inventory and sign for all major and minor equipment upon their assignment to a department.

(2) Maintain accountability of all pagers issued to their department.

(a) Ensure that damaged pagers and pager chargers are returned to Head, Operating Management Department for repair or replacement.

(b) Report all missing, lost, stolen, or recovered pagers immediately to the Security Officer.

(3) Ensure that all doors within their spaces are in good repair and that they are locked when the areas are left unattended and at the end of normal working hours.

(4) Ensure all contractor and vendor personnel are accompanied at all times while performing work.

(5) Maintain and have available, an accurate listing of both minor and plant property assigned to their department for easy identification in case of missing, lost, stolen or recovered (M-L-S-R) government property incidents.

f. OOD and MOD shall:

(l) Make a minimum of 1 security round every 8 hours.

(2) Make exterior rounds of all buildings, structures, facilities, and work spaces, making note of the condition of all barriers and lighting. Report security violations to the Security Officer.

(3) Enter all security infractions, discrepancies, or compromises in the Command Journal.

(4) Ensure only main and emergency entrances to the hospital are open after normal working hours, during the night shift and on weekends.

(a) All external doors of the main building will be secured as needed by mission requirements.

(b) Specific times that individual doors are secured and opened are found in the Intrusion Detection System's Standard Operating Procedures.

(c) Exceptions to this are the Lobby and Emergency Department doors which will remain unlocked at all times.

(d) The OOD may authorize opening doors for special occasions. If authorization is given, the MOD will open and secure the door(s) as directed by the OOD.

(e) The OOD will maintain custody/control of master keys at all times.

g. All personnel will:

(l) Immediately report incidents of theft or abuse to the Security Officer or CMAA.

(2) Be encouraged to make suggestions for improvement in loss control procedures or effective use of material assets to the Security Officer.

(3) All personnel will challenge visitors after hours and direct them to the appropriate ward or department. Notify the ward or department that a visitor is present.

Chapter 9

MISSING, LOST STOLEN, RECOVERED (M-L-S-R) PROGRAM

9001. Purpose. This chapter provides procedures for reporting missing, lost, stolen or recovered (M-L-S-R) government property pursuant to references (b) and (c).

9002. Background

a. The Department of the Navy maintains statistics to determine where, when, and how Navy property is missing, lost, stolen, or recovered in order to improve the Navy's Physical Security Program. Accordingly, M-L-S-R reports can be used by the command to assess the loss prevention program and to take action necessary to correct any real or perceived security deficiencies.

b. The following types of property are included under the M-L-S-R program:

(l) All serialized government property having a value of five hundred dollar ($500.00) or more must be reported using the DD Form 200 (MLSR).

(2) All other unserialized government property considered to be "substantive" regardless of the actual or estimated amount that are not otherwise covered by any other regulation, must be reported using DD Form 200 i.e., medications, immunizations, precious metals, gifts of silver and other valuable articles presented to the command, plus highly technical devices, Information Systems hardware or software, etc.

9003. Definitions

a. Missing. Items which are not in their proper place or cannot be readily accounted for and searches by responsible personnel have been completed without success. The incident has been reported to the Security Officer and loss reporting action has been initiated.

b. Lost. Items that cannot be found and have not been surveyed or otherwise removed from accountability after investigation.

c. Stolen. Items that are not in their proper place or are unaccounted for and evidence indicates theft or other related criminal activity.

d. Recovered. Items that are gained by inventory (GBI), found, or recovered after being reported missing, lost, stolen or suspected to be the remainder of a loss due to theft or fraud.

9004. Action

a. Department Heads shall immediately report to the Security Officer and the Equipment Manager all missing, lost, stolen, or recovered (M-L-S-R) government property, as directed by reference (b).

b. Security Officer shall:

(l) Act in accordance with the procedures and format set forth in enclosure (2) of reference (c).

(2) Conduct initial investigations of loss and request assistance from PMO or NCIS when criminal activity is evident or suspected.

(3) Complete M-L-S-R documentation.

(4) Take specific security measures as indicated by the incident (e.g., none; increased security measures; increased loss prevention measures; improved administrative measures; etc.)

(5) Present M-L-S-Rs to the Loss Prevention Subcommittee for trend analysis and recommendations.

Chapter 10

INTRUSION DETECTION SYSTEM

10001. Purpose. To provide procedures in using the Intrusion Detection System (IDS).

10002. Background. The Naval Hospital employs a proprietary IDS as defined by reference (a). This system is monitored at the Information Desk. It provides for an efficient use of personnel and warning of attempted penetration into protected areas.

10003. Action

a. Security Officer shall:

(l) Conduct monthly testing of the IDS. All sensors must be tested for serviceability and adequacy.

(2) Schedule preventive maintenance as recommended by the IDS's manufacturer.

(3) Immediately respond to an IDS alarm during working hours.

(4) Request military police assistance as dictated by the situation.

(5) Maintain an IDS SOP.

(6) Train watchstanders in the proper use of the IDS monitoring station.

b. OOD or MOD shall:

(l) Immediately respond to all IDS alarms after hours.

(2) Record in the Command Journal a detailed entry containing the alarm site, time, and investigative findings.

c. Naval Hospital personnel shall not modify nor tamper with the IDS without authority from the Security Officer.

Chapter 11

BOMB THREAT PROCEDURES

11001. Purpose. To publish policies and procedures in the event of a bomb threat.

11002. Background. When handling, disarming or disposing of explosive devices or suspected explosive devices, it must be realized that the exterior appearance of a known or suspected device gives little or no indication of the explosive used or the manner of construction. These key factors are largely dependent upon the availability of materials and technical skill of the saboteur. This prevents the establishment of set handling procedures. The primary concern is the safety of life and property.

11003. Action

a. Security Officer/OOD shall:

(l) Notify the Commanding Officer, Executive Officer, Director for Administration and Head, Facilities Management Department and the CDO of the MCAGCC.

(2) Assess the situation based on information received from the caller.

(3) Call PMO, Explosive Ordinance Disposal (EOD) and the Fire Department.

(4) Evacuate and isolate any area the caller may have indicated as a location of a bomb.

(5) Secure all spaces containing suspicious packages(s) and notify PMO.

(6) Secure mattresses or sandbags for use as protective shields and barricades. These protective shields or barricades shall only be used at the direction of Explosive Ordinance Disposal (EOD) personnel.

(7) Notify all inhabitants of the affected building not to use their telephones, cellular phones, radios or any other electronic equipment.

(8) Secure auto traffic in close proximity to the affected building.

(9) Turn operations over to PMO and EOD personnel upon arrival.

b. Head, Facilities Management Department shall shut off power and gas lines leading into the danger area if possible. (If requested by the on-scene commander)

c. Person receiving a bomb threat shall:

(l) Remain calm and keep the caller on the line as long as possible.

(2) Begin recording specifics of conversation and identifiable characteristics of caller using the Bomb Threat Call Checklist. NAVHOSP29PALMS Form 3440/03 (Rev. 2/94), Figure 11-1. The checklist is also located inside the Naval Hospital in-house telephone directory.

(3) Gesture or motion to a co-worker for assistance. When the caller hangs up, dial *33 to have call traced.

d. Co-worker shall notify the Security Officer or Officer of the Day.

e. Person finding a suspicious package shall:

(l) Remain calm and isolate the area.

(2) Request a co-worker to notify the Security Officer or OOD.

f. If the order to evacuate is announced, All Hands will:

(l) Evacuate the building in the same manner as a "fire" evacuation (Code RED).

(2) Remain at their exterior muster site.

(3) Not re-enter the building until the "all clear" is sounded by either the base Fire Department or PMO personnel.

BOMB THREAT CALL CHECKLIST

QUESTIONS TO ASK: EXACT WORDING OF THE THREAT:

1. When is the bomb going to explode? _____
2. Where is it right now? _____
3. What does it look like? _____
4. What kind of bomb is it? _____
5. What will cause it to explode? _____
6. Did you place the bomb? _____
7. Why? _____
8. What is your address? _____
9. What is your name? _____

Sex of caller_____ Age_____ Race _____ Length of call _____

CALLER'S VOICE:

___Calm	___Laughing	_____ Lisp	____Disguised
___Angry	___Crying	_____ Raspy	____Accent
___Excited	___Normal	_____ Deep	____Familiar
___Slow	___Distinct	_____ Ragged	If voice is
___Rapid	___Slurred	_____ Clearing throat	familiar, who
___Soft	___Nasal	_____ Deep breathing	did it sound
___Loud	___Stutter	_____ Cracking voice	like?_____

BACKGROUND SOUNDS:

_____Street noises	_____House Noises	_____Factory machinery
_____Motor	_____Long distance	_____Voices
_____Local	_____Ps system	_____Office machinery
_____Animal noises	_____Music	_____Static
_____Clear	_____Other	

THREAT LANGUAGE:

_____Well spoken (educated)	_____Foul	_____Incoherent
	_____Irrational	_____Taped
	_____Message read by threat maker	

REMARKS:_____
_____
_____
_____

Report call immediately to the SECURITY OFFICER (at extension 2189 or 2872) or the OFFICER OF THE DAY (at extension 2872)

Fill out completely, immediately after a bomb threat.
Date____/____/____Phone number_____
Name_____ Position_____

Figure 11-1

Chapter 12

TERRORIST THREAT CONDITIONS

12001. Purpose. To establish policy, procedures and preventive measures in the event of a terrorist threat condition.

12002. Background. Terrorism is the unlawful use or threatened use of force or violence against individuals or property, with the intention of coercing or intimidating governments or societies often for political, religious or ideological purposes. Acts of terrorism directed at Naval personnel, activities or installations have the potential to destroy critical facilities, injure or kill personnel, impair or delay accomplishment of mission and cause incalculable damage through adverse publicity and public perception of incident handling and results. The record of terrorist activities directed at Naval facilities indicate the use of bombs, ambush, armed attack, hostage situations and sabotage.

12003. Action. Once the decision to arrive at a particular THREATCON is made by the Commanding General the Security Officer shall enforce the following Terrorist Threat Conditions, and their associated security measures as follows:

a. THREATCON NORMAL applies when a general threat of possible terrorist activity exists, but warrants only a routine security posture.

b. THREATCON ALPHA applies when there is a general threat of possible terrorist activity against the Naval Hospital, MCAGCC or any associated personnel. The nature and extent is unpredictable, and circumstances do not justify full implementation of THREATCON BRAVO measures. Below lists preventive security measures, but does not limit the use of intelligence received or as a deterrent.

(l) MEASURE 1. Remind all personnel at regular intervals, including family members, to be suspicious and inquisitive about strangers, particularly those carrying suitcases or other containers. Be alert for unidentified vehicles in the vicinity of the Naval Hospital or Military Sickcall. Be alert for abandoned parcels or suitcases or any unusual activity.

(2) MEASURE 2. Keep available at all times for the OOD, plans for evacuating or sealing off the buildings and/or any area in use or where an explosion or attack has occurred. Keep key personnel who may be needed to implement security plans on call.

(3) MEASURE 3. Secure buildings and all rooms and storage areas not in regular use.

(4) MEASURE 4. As a deterrent, apply one of the following measures from THREATCON BRAVO individually and randomly:

(a) Secure and regularly inspect building and all rooms and storage areas not in use.

(b) At the beginning of each workday and at regular and frequent intervals, inspect the interior and exterior of the building for suspicious packages or activities.

(c) Check all deliveries to the buildings. Advise family members to check all home deliveries.

(5) MEASURE 5. Review all plans, orders, personnel details, and logistic requirements related to the introduction of a higher THREATCON.

(6) MEASURE 6. As appropriate, review and implement security measures for high-risk personnel.

(7) MEASURE 7. As appropriate, consult MCAGCC law enforcement personnel on the threat and mutual antiterrorist, (AT), measures.

(8) MEASURE 8 - 10. Reserved for future use.

c. THREATCON BRAVO. Applies when increased and more predictable threat of terrorist activity exist.

(1) MEASURE 11. Repeat measure 1 in paragraph 2.a., above, and warn personnel of any terrorist form of attack.

(2) MEASURE 12. Keep all personnel involved in implementing antiterrorist contingency plans on call.

(3) MEASURE 13. Check plans for implementation of the measures in the next higher THREATCON.

(4) MEASURE 14. Where possible, cars and objects such as crates, trash containers, etc., are to be moved at least 25 meters from buildings.

(5) MEASURE 15. Secure and regularly inspect the buildings, all rooms and storage areas that are not in regular use.

(6) MEASURE 16. At the beginning and end of each workday and at other regular and frequent intervals, inspect the interior and exterior of the building for suspicious packages.

(7) MEASURE 17. Examine all mail for letter or parcel bombs.

(8) MEASURE 18. Check all deliveries to the building.

(9) MEASURE 19. Increase surveillance of buildings and all associated areas.

(10) MEASURE 20. Make all staff personnel and their dependents aware of the general situation in order to stop rumors and to prevent unnecessary alarm.

(11) MEASURE 21. At an early stage, inform all Department Heads and any other key personnel of any action being taken and why.

(12) MEASURE 22. On entry of visitors to the facility, visually inspect all, and randomly inspect a percentage of their suitcases, parcels, and other containers.

(13) MEASURE 23. If possible, and utilizing Naval Hospital, Security personnel, operate random security patrols to check vehicles, people, buildings, and the surrounding areas.

(14) MEASURE 24. Protect military transport vehicles in accordance with prepared plans. Remind duty drivers to lock parked vehicles and to institute a positive system of checking before they enter and drive the vehicle.

(15) MEASURE 25. Implement additional security measures for high-risk personnel, as appropriate.

(16) MEASURE 26. As appropriate, consult MCAGCC law enforcement personnel on the threat and mutual AT measures.

(17) MEASURE 27 - 29. Reserved for future use.

d. THREATCON CHARLIE. Applies when an incident occurs or intelligence is received indicating some form of terrorist action against personnel of the Naval Hospital.

(l) MEASURE 30. Continue all THREATCON BRAVO measures or complete those that are pending.

(2) MEASURE 31. Keep available, at their place of duty, all personnel who are responsible for implementing AT plans.

(3) MEASURE 32. Limit access points to an absolute minimum.

(4) MEASURE 33. Strictly enforce control of entry and search a percentage of all packages or containers.

(5) MEASURE 34. Enforce centralized parking of vehicles.

(6) MEASURE 35. Increase security patrolling of the building and surrounding areas.

(7) MEASURE 36 - 39. reserved for future use.

e. THREATCON DELTA. Implementation applies in the immediate area where a terrorist attack has occurred or when intelligence has been received that a terrorist action against a specific location is likely. Normally, that THREATCON is declared as a localized warning.

(l) MEASURE 41. Continue or introduce <u>all</u> measures listed for THREATCON BRAVO and CHARLIE.

(2) MEASURE 42. Control access and implement positive identification of all personnel.

(3) MEASURE 43. Search all suitcases, briefcases, packages, etc., that are brought into the hospital or Military Sick Call.

(4) MEASURE 44. Take measures to control access to all areas under the jurisdiction of the Naval Hospital.

(5) MEASURE 45. Make frequent security inspections of the exterior of all building and of all parking areas.

(6) MEASURE 46. Minimize all administrative journeys and visits.

(7) MEASURE 47 - 50. Reserved for future use.

Chapter 13

Infant Security Procedures

13001. Purpose. To establish policy and procedures for the safety and security of new born infants and pediatric patients during their inpatient stay at Naval Hospital, Twentynine Palms.

13002. Background. Infant kidnappings in the hospital setting have occurred with increasing frequency over the course of the past decade. This procedure is designed to provide guidance for minimizing the risk of this incident occurring at this command. Although electronic surveillance systems are very useful in helping to deter an infant abduction, the *BEST SECURITY IS THE STAFF MEMBERS WORKING IN THE MATERNAL INFANT NURSING DEPARTMENT USING THEIR EYES AND EARS!*

13003. ACTION

a. Maternal Infant Nursing Department (MIND) Staff will:

(1) Wear Photo Identification Badges with yellow highlighted information at all times.

(2) Inform parents not to allow anyone to take their infant from the room without first identifying themself and who does not have photo ID visable with the yellow highlighted information.

(3) Establish enternal policy for identifying mother, infant and father.

(4) Approach visitors who appear to be lost in the MIND area and offer assistance and direct them to the appropriate place.

(5) Be extremely caucious of an individual who identifies themself as a provider or technician, and the staff member does not recognize the individual as a member of the Naval Hospital staff. The staff member must ask for positive identification. Be suspicious of unidentified “visitors” asking questions regarding hospital routines, or security policies.

(6) Be vigilant to the presence of visitors to the area. Notify Hospital Security at extension 2190 if there appears to be suspicious or unusual activity observed by visitors to this area.

b. In the event of an abduction or an attempt, the following procedures shall be followed:

(1) Nursing staff:

(a) Notify hospital security by calling 2190 and inform them of the incident. Request that a “Code Pink” announcement be made on the overhead.

(b) Search the MIND and obtain a head count of all infants.

(2) Hospital Security and Administration:

(a) “Code Pink” shall be announced over the Public Address System immediately.

(b) The Provost Marshals Office (PMO) shall be notified by calling 9-1-1.

(c) All other area hospitals and clinics shall be notified and a complete description of the infant and abductor, if known, shall be provided.

(3) Upon hearing the “Code Pink” announcement, *all staff members* will participate in a hospital wide search of the hospital and grounds. All exits shall be sealed, and all suspicious acts shall be reported to hospital security at extension 2190. Time is of essence as the abductor may not have left the premises.

(4) Upon hearing the “Code Pink” announcement, each department head will immediately dispatch a person to all identified exits with the instructions to verify the identity (using picture identification) of all persons leaving the facility. Military personnel and their dependents are required to posses their ID cards at all times. Exit monitors will not unlawfully detain any person. They will explain the crisis and ask for each persons cooperation as they depart the building.

(5) Search all restrooms, storage rooms and office spaces where an abductor could be hiding or could have placed the infant. Report all suspicious acts to hospital security at extension 2190.

(6) After normal working hours, the duty personnel will monitor the main entrance of the hospital, and immediately respond to alarmed exit. The Emergency Medicine Department Staff will monitor the exit at the patient entrance.

CODE PINK DRILL CHECKLIST

(Revised 8/27/98)

DATE:_____ TIME:_____

DEPARTMENT:_____ LOCATION: _____

PRE-DRILL

__Department knows assigned door
___Department has watchbill assigning doors on a rotational basis
___Department knows to report suspicious acts to quarterdeck at extension# 2190
___Department has logged “Code Pink” training in individual competency files

DURING DRILL

___Department sends people to cover their assigned door (which is: _____
___Department response is timely
___Department checks all rooms in their area
___Nursing personnel obtains headcount of all infants/children
___Description of child is obtained
___Detailed information is relayed to quarterdeck

EXIT WATCH

___Exit watch arrives in a timely manner
___Exit watch has writing materials to record descriptions of infant, person or vehicle
___Exit watch checks picture ID for each person leaving hospital
___Exit watch explains to each person the nature of the crises and asks for cooperation
___Exit watch knows not to unlawfully detain any person
___Exit watch knows not to leave post until properly relieved

QUARTERDECK

___Quarterdeck announces “Code Pink (EVENT OR DRILL) in progress” properly over public address system
___Quarterdeck records accurate information regarding the child
___Quarterdeck calls PMO and properly informs them of “Code Pink”
___Quarterdeck notifies all other hospitals and clinics of situation

POST DRILL

___Department conducts critique
___Department sets goals for improvement
___Department fills out training roster (NH Form 1500/08) and forwards copy to Ed/Trng

(After 10/01/97, A copy of a checklist with negative responses shall be forwarded to Director)

Figure 13-1

CHAPTER 14

CLASSIFIED INFORMATION AND PERSONNEL SECURITY PROGRAM

14001. Purpose. To publish policies and procedures for the information and personnel security program.

14002. Policy. This program is established to ensure that classified information is protected from unauthorized disclosure. Appointment of military and civilian employees granted access to classified information or assignment to other sensitive duties will be clearly consistent with the interests of national security, as directed by reference (h).

14003. Action

a. The Commanding Officer shall:

(l) Have ultimate responsibility for effective management of the Information and Personnel Security program.

(2) Appoint in writing the Command Security Manager, Top Secret Control Officer, Personnel Security Officer, and the Classified Material Control Officer.

b. The Security Manager shall:

(l) Be the principal advisor on information and personnel security in the Command and is responsible to the Commanding Officer for the management of the program.

(2) Have a secret clearance with a background investigation.

c. The Personnel Security Officer (PSO) shall:

(l) Have a secret clearance.

(2) Ensure all personnel who are to handle classified information or to be assigned to sensitive duties are appropriately cleared and that requests for personnel security investigations are properly prepared, submitted and monitored.

(3) Ensure a list is maintained of personnel granted access to classified material for the Command on a need-to-know basis.

(4) Ensure Classified Information Nondisclosure Agreement is signed upon final notification of clearance granted.

(5) Ensure each person who will have access to classified information be given an orientation briefing as soon as possible after reporting aboard or being assigned to duties involving classified access.

(6) Ensure security clearances are monitored to not exceed the level required to performed assigned duties.

(7) Ensure all security awareness training is conducted on a timely basis per reference (h).

(8) Brief and debrief personnel with clearances travel-ing to foreign countries whether it be official or personal.

(9) Maintain records of personal foreign travel reported by assigned personnel. These records should identify, whenever possible, the travellers route and mode of travel, destination, length of stay, identity of fellow travellers (when accompanying the traveller) and identity of tour operators (if a tour operator is used).

d. Classified Material Control Officer shall:

(l) Have a secret clearance.

(2) Maintain the Command Classified Container ensuring all classified material is accounted for before securing.

(3) Ensure compliance with accounting and control requirements for classified material, including receipt, distri-bution, inventory, reproduction and disposition.

(4) Conduct an annual inventory of all classified material held in the command.

(5) Ensure the combination is changed when containers/ locks are first placed in use, at least annually thereafter, when an individual knowing the combination no longer requires access or if the combination has been subject to possible compromise.

(6) Ensure that the security container is secure and checked before departing for the day.

(7) Ensure that an Emergency Removal Plan exists in the case of a disaster.

e. The Top Secret Control Officer shall:

(l) Have a Top Secret clearance.

(2) Maintain a system of accountability.

(3) Transmit Top Secret material within the Command by direct personal contact.

(4) Maintain a current roster of persons within the Command who are authorized access to Top Secret information.

(5) Ensure no Top Secret material is stored at this Command.

f. Directors or Department Heads

(l) With Safes/Containers in their areas shall:

(a) Ensure no storage of classified material.

(b) Ensure Security Officer receives SF-700, Security Container Information Card upon change of combination.

(2) Shall ensure that those persons requesting leave or TAD outside CONUS or its territories route their requests through the Personnel Security Officer. These individuals are to receive a foreign travel brief two to four weeks prior to departing the command.

g. All Staff Personnel shall adhere to security regulations established within the command whether they have a clearance or not. If anything looks suspicious or questionable, report the incident to the Security Officer or the Officer of the Day.